PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute fo	or form 1449A/P1	ro	•	Complete if Known		
				Application Number	10/765,976	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT			LOSURE	Filing Date	January 29, 2004	
			PLICANT	First Named Inventor	VANSTONE	
(use as many sheets as necessary)				Art Unit	NOT YET SPECIFIED	
				Examiner Name	NOT YET SPECIFIED	
Sheet	1	of	2	Attorney Docket Number	T00001-0378-US1	

	U.S. PATENT DOCUMENTS						
Examiner Initials	Cite No.1	Document Number Number Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear		
1		US- 5,146,500	09-08-1992	MAURER			
1		US- 5,159,632	10-27-1992	CRANDALL			
		US- 5,271,061	12-14-1993	CRANDALL			
		US- 5,272,755	12-21-1993	MIYAJI et al.			
M		US- 5,351,297	09-27-1994	MIYAJI et al.			
97		US- 5,442,707	08-15-1995	MIYAJI et al.			
		US- 5,463,690	10-31-1995	CRANDALL			
		US- 5,497,423	03-05-1996	MIYAJI			
4		US-					
		US-					
		us-					
		US-					
		US-					
		US-					
		US-					
		US-					
		US-					
		US-					
		US-					
		US-					

	FOREIGN PATENT DOCUMENTS							
Examiner Initials*	Cite No.1	Foreign Patent Document			Publication Date	Name of Patentee or	Pages, Columns, Lines, Where Relevant	
		Office ³	Number ⁴	Kind ⁵ (if known)	MM-DD-YYYY	Applicant of Cited Document	Passanas of Palayant	Т
						•		
								L
	ĺ							

Examiner Signature	Date Considered	270405

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

PTC/SB/08B (08-03)
Approved for use through 08/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

O	, ,	;; \	1
APR	2 0	2004	, Loc
ZR.	DE	A ES	9

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Substitute for form 1449B/PTO

Examiner

Signature

(use as many sheets as necessary)
Sheet 2 of 2

Complete if Known				
Application Number	10/765,976			
Filing Date	January 29, 2004			
First Named Inventor	VANSTONE			
Art Unit	NOT YET SPECIFIED			
Examiner Name	NOT YET SPECIFIED			
Attorney Docket Number	T00001-0378-US1			

		OTHER PRIOR ART NON PATENT LITERATURE DOCUMENTS	
Examiner Initials	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T2
B		KOBLITZ, "CM-Curves with Good Cryptographic Properties", Advances in Cryptology. Santa Barbara, Aug. 11-15, 1991, Proceedings of the Conference on Theory and Applications of Cryptographic Techniques, Berlin, Springer, DE, 1991, pages 279-287.	
B		MEIER W ET AL, "Efficient Multiplication on Certain Nonsupersingular Elliptic Curves", Advances in Cryptology. Santa Barbara, Aug. 16-20, 1992, Proceedings of the Annual International Cryptology Conference, Berling, Springer, DE, vol. CONF. 12, pages 333-344.	
B		SCHOOF R, "Elliptic Curves over Finite Fields and the Computation of Square Roots Mod P", Mathematics of Computation, American Mathematical Society, US, vol. 44, no. 169/170, April 1985, pages 483-494.	
19		LAY G-J ET AL, "Constructing Elliptic Curves with Given Group Order Over Large Finite Fields", Algorithmic Number Theory, International Symposium, 1994, pages 250-263.	
B		MUELLER V, "Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two", PUBLICATIONS, TU DARMSTADT, 1997	
b		SCHNEIER, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 1994, pages 39-41, John Wiley & Sons, New York.	
	_		
L			L_

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

Date

Considered

2JU405

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.